ABSTRACT

A system and method uses a common key provided to a first wireless unit and a second wireless unit to use in secure communications between the first and second wireless units over at least one wireless communications system. By providing a common key to the first and second wireless units, the common key security system alleviates the at least one wireless communications system from having to perform the security methods used to provide secure communications between the first and second wireless units. For example, the encryption/decryption of the communications between the first wireless unit and the second wireless unit can be performed at the first and second wireless units using the common key. In certain embodiments, the first and second wireless units and the serving wireless communications system(s) still perform authentication and obtain keys CK_1 and CK_2 as described above. However, instead of using the keys CK_1 and CK_2 to encrypt/decrypt communications between the first and second wireless units at the serving wireless communications system(s), a common key at the first wireless unit is used to encrypt/decrypt information which is decrypted/encrypted at the second wireless unit using the common key. The common key can be generated by the wireless communications system(s) and provided to the first and second wireless units by the serving wireless communications system(s) which can use the respective keys CK_1 and CK_2 to securely provide the common key to the first and second wireless units. Once the receipt of the common key by the first and second wireless units is verified, the first and second wireless units can securely communicate with each other using the common key, and the serving wireless communications system(s) can simply act as a conduit for the communications between the first and second wireless units.